

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2002-259108**

(43)Date of publication of application : **13.09.2002**

(51)Int.Cl.

G06F 3/12  
B41J 29/00  
B41J 29/38  
G06F 15/00  
H04L 9/32

**(21)Application number : 2001-059015**

(71)Applicant : **CANON INC**

(22)Date of filing : 02.03.2001

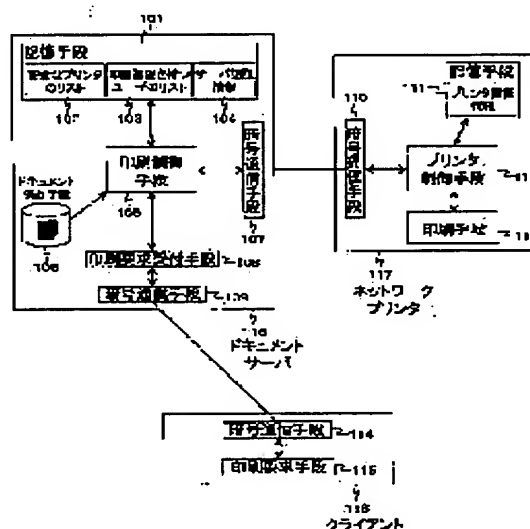
(72)Inventor : HISAMOTO SHINJI  
KATO EIJI

**(54) PRINTING SYSTEM, PRINTER, PRINTING METHOD, RECORDING MEDIUM, AND PROGRAM**

**(57)Abstract:**

**PROBLEM TO BE SOLVED:** To prevent an illegal printer from pretending as a legal printer and to print out data only from a safe printer.

**SOLUTION:** The printing system constituted of a document server, a printer and a user client which are connected through a network stores a disclosed key certificate and a secret key corresponding to the certificate and executes printer certification on the basis of the certification in accordance with a request from the document server or the user client.



## LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

**[Date of final disposal for application]**

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's  
decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号  
特開2002-259108  
(P2002-259108A)

(43) 公開日 平成14年9月13日 (2002.9.13)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テーマコード*(参考)
G 0 6 F 3/12		G 0 6 F 3/12	K 2 C 0 6 1
B 4 1 J 29/00		B 4 1 J 29/38	Z 5 B 0 2 1
29/38		G 0 6 F 15/00	3 3 0 C 5 B 0 8 5
G 0 6 F 15/00	3 3 0	B 4 1 J 29/00	Z 5 J 1 0 4
H 0 4 L 9/32		H 0 4 L 9/00	6 7 3 A
審査請求 未請求 請求項の数21 O L (全 19 頁)			

(21) 出願番号 特願2001-59015(P2001-59015)

(22) 出願日 平成13年3月2日(2001.3.2)

(71) 出願人 000001007

キヤノン株式会社  
東京都大田区下丸子3丁目30番2号

(72) 発明者 久本 慎二

東京都大田区下丸子3丁目30番2号 キヤ  
ノン株式会社内

(72) 発明者 加藤 英二

東京都大田区下丸子3丁目30番2号 キヤ  
ノン株式会社内

(74) 代理人 100090273

弁理士 國分 孝悦

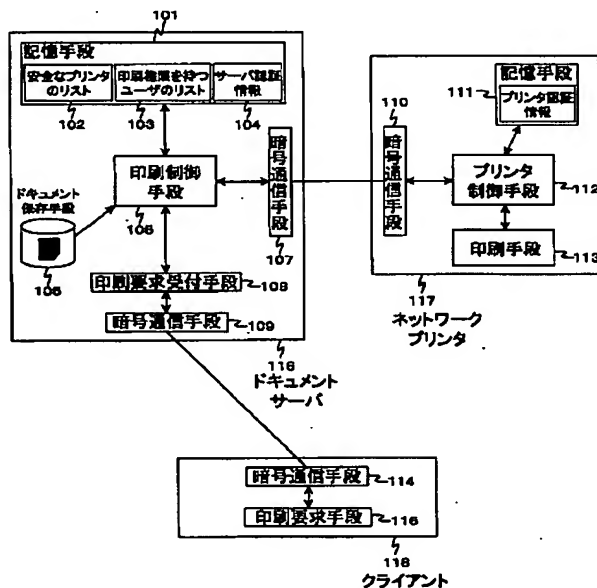
最終頁に続く

(54) 【発明の名称】 印刷システム、印刷装置、印刷方法、記録媒体及びプログラム

(57) 【要約】

【課題】 プリンタのなりすましを防止し、安全なプリンタへのみ印刷することを課題とする。

【解決手段】 本発明の印刷システムは、ネットワークで接続されたドキュメントサーバ、プリンタ、ユーザクライアントから構成される印刷システムであって、プリンタは公開鍵証明書とこれに対応する秘密鍵とを保有し、ドキュメントサーバもしくはユーザクライアントからの要求に応じて公開鍵証明書に基づくプリンタ認証を行う。



【特許請求の範囲】

【請求項1】 ネットワークで接続されたドキュメントサーバ、プリンタ、ユーザクライアントから構成される印刷システムであって、

プリンタは公開鍵証明書とこれに対応する秘密鍵とを保有し、ドキュメントサーバもしくはユーザクライアントからの要求に応じて公開鍵証明書に基づくプリンタ認証を行うことを特徴とする印刷システム。

【請求項2】 前記ドキュメントサーバは内蔵する機密情報と対応づけられた印刷許可プリンタのリストを保有し、印刷要求が行われた際に出力先のプリンタが前記許可プリンタのリストに含まれるかどうかに応じて前記出力先のプリンタに印刷データを送信することを特徴とする請求項1に記載の印刷システム。

【請求項3】 前記プリンタの公開鍵証明書は、前記プリンタの安全性を示す情報を含み、前記ドキュメントサーバは内蔵する機密情報と対応づけられた印刷許可プリンタの安全性を示す情報のリストを保有することを特徴とし、印刷要求が行われた際に出力先のプリンタの公開鍵証明書による認証を行い、前記プリンタが前記ドキュメントサーバの保有する許可プリンタの安全性を示す情報のリストに記された条件を満足するかどうかに応じて、前記出力先のプリンタに印刷データを送信することを特徴とする請求項1に記載の印刷システム。

【請求項4】 公開鍵証明書とこれに対応する秘密鍵とを保有し、外部からの要求に応じて公開鍵証明書に基づくプリンタ認証を行うことを特徴とする印刷装置。

【請求項5】 内蔵する機密情報と対応づけられた印刷許可プリンタのリストを保有し、印刷要求が行われた際に出力先のプリンタが前記印刷許可プリンタのリストに含まれるかどうかに応じてドキュメントサーバから送信された印刷データの印刷を行うことを特徴とする印刷装置。

【請求項6】 公開鍵証明書とこれに対応する秘密鍵とを保有し、外部からの要求に応じて公開鍵証明書に基づくプリンタ認証を行うステップを有することを特徴とする印刷方法。

【請求項7】 内蔵する機密情報と対応づけられた印刷許可プリンタのリストを保有し、印刷要求が行われた際に出力先のプリンタが前記印刷許可プリンタのリストに含まれるかどうかに応じて、前記出力先のプリンタに印刷データを送信するステップを有することを特徴とする印刷方法。

【請求項8】 公開鍵証明書とこれに対応する秘密鍵とを保有し、外部からの要求に応じて公開鍵証明書に基づくプリンタ認証を行う手順をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項9】 内蔵する機密情報と対応づけられた印刷許可プリンタのリストを保有し、印刷要求が行われた際

に出力先のプリンタが前記印刷許可プリンタのリストに含まれるかどうかに応じて、前記出力先のプリンタに印刷データを送信する手順をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項10】 公開鍵証明書とこれに対応する秘密鍵とを保有し、外部からの要求に応じて公開鍵証明書に基づくプリンタ認証を行う手順をコンピュータに実行させるためのプログラム。

【請求項11】 内蔵する機密情報と対応づけられた印刷許可プリンタのリストを保有し、印刷要求が行われた際に出力先のプリンタが前記印刷許可プリンタのリストに含まれるかどうかに応じて、前記出力先のプリンタに印刷データを送信する手順をコンピュータに実行させるためのプログラム。

【請求項12】 ネットワークで接続されたドキュメントサーバ、プリンタ、ユーザクライアントから構成され、前記プリンタを経由する参照印刷を行う印刷システムであって、

印刷を行う機密情報の印刷権限を確認するため使用される印刷要求データの少なくとも一部を、前記ドキュメントサーバでのみ復号可能なように前記ユーザクライアントにおいて暗号化し送付することを特徴とする印刷システム。

【請求項13】 前記ドキュメントサーバにおけるユーザ認証方式がユーザの公開鍵証明書に基づく認証であって、ユーザの公開鍵証明書にはユーザのアクセス権を示すクラス名が記載されており、前記ドキュメントサーバにおける印刷権限の確認がこのユーザの公開鍵証明書に記載されているクラス名に基づいて行われることを特徴とする請求項12に記載の印刷システム。

【請求項14】 印刷を行う機密情報の印刷権限を確認するため使用される印刷要求データの少なくとも一部を、ドキュメントサーバでのみ復号可能なように暗号化しプリンタ経由で前記ドキュメントサーバに送信することを特徴とする印刷装置。

【請求項15】 プリンタ経由でユーザから印刷要求データを受信する受信手段と、

前記印刷要求データに基づくユーザ認証方式がユーザの公開鍵証明書に基づく認証であって、ユーザの公開鍵証明書にはユーザのアクセス権を示すクラス名が記載されており、ドキュメントサーバにおける印刷権限の確認がこのユーザの公開鍵証明書に記載されているクラス名に基づいて行う認証手段とを有することを特徴とする印刷装置。

【請求項16】 印刷を行う機密情報の印刷権限を確認するため使用される印刷要求データの少なくとも一部を、ドキュメントサーバでのみ復号可能なように暗号化しプリンタ経由で前記ドキュメントサーバに送信するステップを有することを特徴とする印刷方法。

【請求項17】 プリント経由でユーザから印刷要求データを受信する受信ステップと、  
前記印刷要求データに基づくユーザ認証方式がユーザの公開鍵証明書に基づく認証であって、ユーザの公開鍵証明書にはユーザのアクセス権を示すクラス名が記載されており、ドキュメントサーバにおける印刷権限の確認がこのユーザの公開鍵証明書に記載されているクラス名に基づいて行う認証ステップとを有することを特徴とする印刷方法。

【請求項18】 印刷を行う機密情報の印刷権限を確認するため使用される印刷要求データの少なくとも一部を、ドキュメントサーバでのみ復号可能なように暗号化しプリント経由で前記ドキュメントサーバに送信する手順をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項19】 プリント経由でユーザから印刷要求データを受信する受信手順と、  
前記印刷要求データに基づくユーザ認証方式がユーザの公開鍵証明書に基づく認証であって、ユーザの公開鍵証明書にはユーザのアクセス権を示すクラス名が記載されており、ドキュメントサーバにおける印刷権限の確認がこのユーザの公開鍵証明書に記載されているクラス名に基づいて行う認証手順をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項20】 印刷を行う機密情報の印刷権限を確認するため使用される印刷要求データの少なくとも一部を、ドキュメントサーバでのみ復号可能なように暗号化しプリント経由で前記ドキュメントサーバに送信する手順をコンピュータに実行させるためのプログラム。

【請求項21】 プリント経由でユーザから印刷要求データを受信する受信手順と、  
前記印刷要求データに基づくユーザ認証方式がユーザの公開鍵証明書に基づく認証であって、ユーザの公開鍵証明書にはユーザのアクセス権を示すクラス名が記載されており、ドキュメントサーバにおける印刷権限の確認がこのユーザの公開鍵証明書に記載されているクラス名に基づいて行う認証手順をコンピュータに実行させるためのプログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ドキュメントサーバ上で管理されている機密性を含むドキュメントを、ネットワークに接続されたプリンタに対して、安全に印刷する技術に関するものである。

【0002】

【従来の技術】近年、インターネットとWEB技術の普及によって、WEBサーバでドキュメントを公開することが広く行われている。企業内などのイントラネットにおいても、同様にWEBサーバを用いてドキュメントの

管理・公開が行われており、機密性を含むドキュメントについてもこれと共通した環境での安全な運用が求められている。

【0003】特定のプロトコルやサーバではなく、一般的にドキュメントサーバ、ネットワークプリンタと、ユーザが印刷を指示するクライアントがネットワークで接続されている形態を考える。

【0004】これらを用いて、ユーザが印刷を指示し、ドキュメントのデータがネットワークプリンタに送られる経路を考えると図22（印刷の形態）のような印刷の形態が考えられる。

【0005】図22aのクライアント印刷は、通常ウェブブラウザなどのアプリケーションによってドキュメントを表示・印刷するときの形態である。また、図22bのサーバ印刷は、クライアントからの印刷指示にもとづきサーバ上で印刷のためのプロセスを起動することで印刷を行う形態である。最後に、図22cの参照印刷は、クライアントがネットワークプリンタにドキュメントの所在情報を含む印刷指示を行い、ネットワークプリンタが自らドキュメントサーバにデータを要求して印刷を行う形態である。

【0006】このようなドキュメントサーバ、ネットワークプリンタ、クライアントによって構成される機密情報印刷システムにおいて、ドキュメントサーバ上に管理されているドキュメントを印刷しようとする場合、上記クライアント印刷の図を例にとると、一般に、図23（機密情報印刷の危険）のようなセキュリティ上の危険がある。

【0007】図中、指摘されているものを簡単に説明する。ドキュメントサーバでは、サーバ自体への不正侵入によって、ドキュメントが漏洩したり、破壊・改竄される危険がある。各要素を結ぶ通信路のそれぞれでは、盗聴による漏洩の危険がある。

【0008】ネットワークプリンタでは、印刷後のドキュメントの盗難やコピーが行われる危険がある。またネットワークプリンタ自体を悪意のソフトウェアによって模倣しドキュメントそのものや印刷イメージをそっくりコピーされる危険がある。また、ネットワークプリンタ自体は本物であっても、物理的なつなぎ替え、もしくはネットワーク経路の操作によって、PCやワークステーションを経由して印刷を行うようにし、その間にデータをコピーしたり改竄が行われる危険もある。

【0009】さらにドキュメントにアクセスできるユーザをコントロールしていないのは論外であるが、ユーザ情報（パスワードなど）が盗まれたり、ログインしたままのPCを使われて、そのユーザの権限でドキュメントが閲覧・印刷されてしまうという危険もある。

【0010】ドキュメントを管理する立場からは、このクライアント印刷の形態は、印刷が行われるネットワークプリンタとドキュメントサーバとの接触がないため

に、ネットワークプリンタのなりすましがおこなわれていないか確認する手段がないことも問題である。また、この形態では、ドキュメントデータが必ずクライアントのPCを経由するため、PCローカルのコピーや途中のWEBプロキシ上のキャッシュデータからの漏洩を防止しづらいことも問題である。

【0011】これ以外にも、ドキュメントサーバのなりすましによる偽情報の流布や、偽のネットワーク情報（DNSなど）によるなりすましなど、機密情報の印刷には多数の危険がある。

【0012】上記の危険のうち、通信路の盗聴、およびドキュメントサーバ（WEBサーバ）のなりすましについては、暗号通信と認証のミドルウェアである、SSL（Secure Sockets Layer: Netscape Communications Corporation, USP No. 5657390, <http://www.netscape.com/eng/ss13/draft302.txt>）や、TLS（Transport Layer Security: IETF (Internet Engineering Task Force), RFC 2246, <http://www.ietf.org/rfc/rfc2246>）を用いることによって、WEBサーバをSSL対応とし、WEBブラウザからの接続時にWEBサーバの認証（オプションでクライアントの認証）と暗号通信を行い、その危険を防止することが広く行われている。

【0013】これらでも利用されている、より一般的な技術としては、「公開鍵暗号による暗号化と復号」、「デジタル署名」、「公開鍵証明書に基づく認証」および暗号化通信があげられる。むろんこれらは特定のネットワークプロトコルに制約されることはない。これらの技術について、ここで説明することは省くが、（岡本栄司著、暗号理論入門、共立出版株式会社）や、（岡本龍明、山本博資著、現代暗号、産業図書）などに詳しい解説がある。

【0014】なお、図23（機密情報印刷の危険）のドキュメントサーバへの不法侵入による盗み見や改竄および印刷後の盗難の各危険については、システムおよびOS毎の対応やハードウェア的なサポートなどの別種の対応が必要となるので、以下では言及しない。

【0015】

【発明が解決しようとする課題】上記「従来の技術」にあげた機密情報印刷のセキュリティ上の危険の内、印刷に先立ってネットワークプリンタがなりすまされていないか確認する「プリンタの認証」は通常行われていない。

【0016】また、プリンタの認証によってなりすましが行われていないことは確認できても、そのネットワークプリンタが当該文書を印刷するのに適したセキュリテ

ィ機能を持っていたり、適切な運用が行われているとは限らないので、それらが確認されたプリンタ（以下、安全なプリンタ）だけに印刷データを送るようにしなければならない。

【0017】また、機密情報印刷のセキュリティ上の危険以外に、前記参照印刷の形態においては、ユーザ認証情報は必ずネットワークプリンタを経由してドキュメントサーバに送られるため、通信路の盗聴やネットワークプリンタのなりすましによってユーザ認証情報を不正に得、これを再使用することによりドキュメントを再取得したり、他のドキュメントのアクセスにこのユーザ認証情報を流用するという危険が存在する。

【0018】本発明の目的は、上述のように、ネットワークプリンタのなりすましを防止し、安全なプリンタのみへの印刷を可能とすることである。

【0019】本発明の他の目的は、上記の危険を防止するため、参照印刷の形態において、ネットワークプリンタを経由してドキュメントサーバに送られるユーザ認証情報が他の目的に使用できないようにすることである。

【0020】

【課題を解決するための手段】本発明の一観点によれば、ネットワークで接続されたドキュメントサーバ、プリンタ、ユーザクライアントから構成される印刷システムであって、プリンタは公開鍵証明書とこれに対応する秘密鍵とを保有し、ドキュメントサーバもしくはユーザクライアントからの要求に応じて公開鍵証明書に基づくプリンタ認証を行うことを特徴とする印刷システムが提供される。

【0021】本発明の他の観点によれば、公開鍵証明書とこれに対応する秘密鍵とを保有し、外部からの要求に応じて公開鍵証明書に基づくプリンタ認証を行うことを特徴とする印刷装置が提供される。

【0022】本発明のさらに他の観点によれば、内蔵する機密情報と対応づけられた印刷許可プリンタのリストを保有し、印刷要求が行われた際に出力先のプリンタが前記印刷許可プリンタのリストに含まれるかどうかに応じてドキュメントサーバから送信された印刷データの印刷を行うことを特徴とする印刷装置が提供される。

【0023】本発明のさらに他の観点によれば、公開鍵証明書とこれに対応する秘密鍵とを保有し、外部からの要求に応じて公開鍵証明書に基づくプリンタ認証を行うステップを有することを特徴とする印刷方法が提供される。

【0024】本発明のさらに他の観点によれば、内蔵する機密情報と対応づけられた印刷許可プリンタのリストを保有し、印刷要求が行われた際に出力先のプリンタが前記印刷許可プリンタのリストに含まれるかどうかに応じて、前記出力先のプリンタに印刷データを送信するステップを有することを特徴とする印刷方法が提供される。

【0025】本発明のさらに他の観点によれば、公開鍵証明書とこれに対応する秘密鍵とを保有し、外部からの要求に応じて公開鍵証明書に基づくプリンタ認証を行う手順をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体が提供される。

【0026】本発明のさらに他の観点によれば、内蔵する機密情報と対応づけられた印刷許可プリンタのリストを保有し、印刷要求が行われた際に出力先のプリンタが前記印刷許可プリンタのリストに含まれるかどうかに応じて、前記出力先のプリンタに印刷データを送信する手順をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体が提供される。

【0027】本発明のさらに他の観点によれば、公開鍵証明書とこれに対応する秘密鍵とを保有し、外部からの要求に応じて公開鍵証明書に基づくプリンタ認証を行う手順をコンピュータに実行させるためのプログラムが提供される。

【0028】本発明のさらに他の観点によれば、内蔵する機密情報と対応づけられた印刷許可プリンタのリストを保有し、印刷要求が行われた際に出力先のプリンタが前記印刷許可プリンタのリストに含まれるかどうかに応じて、前記出力先のプリンタに印刷データを送信する手順をコンピュータに実行させるためのプログラムが提供される。

【0029】本発明のさらに他の観点によれば、ネットワークで接続されたドキュメントサーバ、プリンタ、ユーザクライアントから構成され、前記プリンタを経由する参照印刷を行う印刷システムであって、印刷を行う機密情報の印刷権限を確認するため使用される印刷要求データの少なくとも一部を、前記ドキュメントサーバでのみ復号可能なように前記ユーザクライアントにおいて暗号化し送付することを特徴とする印刷システムが提供される。

【0030】本発明のさらに他の観点によれば、印刷を行う機密情報の印刷権限を確認するため使用される印刷要求データの少なくとも一部を、ドキュメントサーバでのみ復号可能なように暗号化しプリンタ経由で前記ドキュメントサーバに送信することを特徴とする印刷装置が提供される。

【0031】本発明のさらに他の観点によれば、プリンタ経由でユーザから印刷要求データを受信する受信手段と、前記印刷要求データに基づくユーザ認証方式がユーザの公開鍵証明書に基づく認証であって、ユーザの公開鍵証明書にはユーザのアクセス権を示すクラス名が記載されており、ドキュメントサーバにおける印刷権限の確認がこのユーザの公開鍵証明書に記載されているクラス名に基づいて行う認証手段とを有することを特徴とする印刷装置が提供される。

【0032】本発明のさらに他の観点によれば、印刷を行う機密情報の印刷権限を確認するため使用される印刷要求データの少なくとも一部を、ドキュメントサーバでのみ復号可能なように暗号化しプリンタ経由で前記ドキュメントサーバに送信するステップを有することを特徴とする印刷方法が提供される。

【0033】本発明のさらに他の観点によれば、プリンタ経由でユーザから印刷要求データを受信する受信ステップと、前記印刷要求データに基づくユーザ認証方式がユーザの公開鍵証明書に基づく認証であって、ユーザの公開鍵証明書にはユーザのアクセス権を示すクラス名が記載されており、ドキュメントサーバにおける印刷権限の確認がこのユーザの公開鍵証明書に記載されているクラス名に基づいて行う認証ステップとを有することを特徴とする印刷方法が提供される。

【0034】本発明のさらに他の観点によれば、印刷を行う機密情報の印刷権限を確認するため使用される印刷要求データの少なくとも一部を、ドキュメントサーバでのみ復号可能なように暗号化しプリンタ経由で前記ドキュメントサーバに送信する手順をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体が提供される。

【0035】本発明のさらに他の観点によれば、プリンタ経由でユーザから印刷要求データを受信する受信手順と、前記印刷要求データに基づくユーザ認証方式がユーザの公開鍵証明書に基づく認証であって、ユーザの公開鍵証明書にはユーザのアクセス権を示すクラス名が記載されており、ドキュメントサーバにおける印刷権限の確認がこのユーザの公開鍵証明書に記載されているクラス名に基づいて行う認証手順をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体が提供される。

【0036】本発明のさらに他の観点によれば、印刷を行う機密情報の印刷権限を確認するため使用される印刷要求データの少なくとも一部を、ドキュメントサーバでのみ復号可能なように暗号化しプリンタ経由で前記ドキュメントサーバに送信する手順をコンピュータに実行させるためのプログラムが提供される。

【0037】本発明のさらに他の観点によれば、プリンタ経由でユーザから印刷要求データを受信する受信手順と、前記印刷要求データに基づくユーザ認証方式がユーザの公開鍵証明書に基づく認証であって、ユーザの公開鍵証明書にはユーザのアクセス権を示すクラス名が記載されており、ドキュメントサーバにおける印刷権限の確認がこのユーザの公開鍵証明書に記載されているクラス名に基づいて行う認証手順をコンピュータに実行させるためのプログラムが提供される。

【0038】本発明によれば、プリンタのなりすましを防止し、安全なプリンタへのみ印刷することができる。また、参照印刷の形態において、プリンタを経由してド

キュメントサーバに送られるユーザ認証情報が他の目的に使用できないようにすることができる。

【0039】

【発明の実施の形態】以下、本発明の実施形態を、実施例に沿って図面を参照しながら説明する。

(第1の実施例) 図1は本発明における第1の実施例の機密情報印刷システムの構成図の構成図である。

【0040】図2はサーバ印刷のプロトコル図、図3はドキュメントサーバ上の印刷制御手段の処理のフローチャート、図4はネットワークプリンタのプリンタ制御手段の処理のフローチャートである。

【0041】図1において、クライアント118は、ユーザによって入力された印刷要求データに従って印刷を行なう印刷要求手段115と、データの暗号化や復号を行ない、サーバと暗号通信を行なうための暗号通信手段114から成る。また、ドキュメントサーバ116は、クライアントからの印刷要求を受け取って印刷制御手段に渡す印刷要求受付手段108と、クライアントに指定されたプリンタを安全であると確認するために照合する安全なプリンタリスト102、印刷を要求するユーザが正当な印刷権限を持っているかを確認するために照合する印刷権限を持つユーザのリスト103、サーバの公開鍵証明書とサーバの秘密鍵から成るサーバを認証するためのサーバ認証情報104を保有しておく記憶手段101と、ドキュメントを保存しておくための記憶装置であるドキュメント保存手段106と、プリンタの認証及び安全性の確認やユーザの印刷権限の確認、およびドキュメントデータを取り出し印刷データとして送信するといった一連の作業を行なう印刷制御手段105と、クライアントと暗号通信を行なうための暗号通信手段109およびプリンタと暗号通信を行なうための暗号通信手段107から成る。また、ネットワークプリンタ117は、プリンタの公開鍵証明書とプリンタの秘密鍵から成るプリンタを認証するためのプリンタ認証情報を保有する記憶手段111と、サーバの認証を行ない、印刷データを受信して出力装置に渡すプリンタ制御手段112と、サーバと暗号通信を行なうための暗号通信手段110と、印刷データを紙に出力する装置である印刷手段113から成る。

【0042】上述の構成よりなる実施例の動作を、順を追って説明する。本実施例では、前記印刷の形態のうち「サーバ印刷」を例に説明を行なう。

【0043】ユーザはクライアント118の印刷要求手段115を用いて、印刷したいドキュメント、出力したいネットワークプリンタ、そのドキュメントの印刷が許可されているユーザを認証するための情報などの印刷要求データを入力する。印刷したいドキュメントやネットワークプリンタは、例えばWEBサーバ上のURL (Uniform Resource Locator) / URI (Uniform Resource Identifier)

などの形式で行なう。ユーザ認証のための情報としては、例えばユーザ名とパスワードを使用することもできる。

【0044】印刷要求手段115は、次にこれらの印刷要求データを暗号通信手段114およびドキュメントサーバ上の暗号通信手段109を経由して、印刷要求受付手段108に送る。印刷要求受付手段108は、受け取ったデータを印刷制御手段105に渡し、印刷のプロセスが開始される。

【0045】印刷のプロセスの詳細は、図3の印刷制御手段の処理のフローチャートに記されているので、これを参照しながら説明する。

【0046】印刷制御手段105は、受け取った印刷要求データから、ドキュメントを指定する情報(以下、ドキュメントURI)とユーザ認証のための情報を抽出する(S120)。

【0047】次に印刷制御手段105は、ユーザ認証情報に基づいてユーザの認証を行い、さらに印刷権限をもつユーザのリスト103とユーザ名を照合して、当該ドキュメントの印刷権があるか確認する(S121)。ユーザ認証が失敗しているか、印刷権がないと判断(S122のno)された場合には、印刷拒否の通知をクライアント118に行なって(S129)、処理は終了する。ユーザ認証と印刷権が確認(S122yes)された場合は、印刷制御手段105は、印刷要求データから指定された印刷先のネットワークプリンタのURIを取り出し、安全なプリンタのリスト102と照合する(S123)。

【0048】指定されたネットワークプリンタが当該ドキュメントを出力してよいリストに含まれていない場合(S124のno)、印刷拒否の通知をクライアント118に行なって(S130)処理は終了する。指定されたネットワークプリンタが当該ドキュメントを出力してよいリストに含まれている場合(S124のyes)は、次のプリンタの認証に移る。

【0049】本実施例では、プリンタの認証は単独に行なうものではなく、サーバ認証といっしょに行なう形で書かれているが、サーバのなりすましの排除を行わない場合は、サーバ認証を省略した形で行なうこともできる。

【0050】サーバ・プリンタの相互認証は、ドキュメントサーバの暗号通信手段107とネットワークプリンタの暗号通信手段110を経由して、サーバ認証情報104とプリンタ認証情報111を用いた公開鍵証明書に基づく認証を相互に行なうことで実施する。この詳細については、従来の技術にあげた参考文献を参照されたい。

【0051】また、上記の説明で、暗号通信手段114, 109, 107, 110については特に指定しなかったが、従来の技術のSSLやTLSを使用してTCP



／IPによる通信を行なう場合、SSL／TLSでは暗号通信を行なう前にサーバ認証を（オプションとしてクライアント（この場合だとネットワークプリンタ）認証）行なうことができるので、印刷制御手段105での処理を省略することも可能である。

【0052】さて、サーバ・プリンタの相互認証が成功しなかった場合（S126のno）、印刷制御手段105は印刷拒否の通知をクライアントに行なって（S131）処理を終了する。サーバ・プリンタの相互認証が成功した場合（S126のyes）には、ネットワークプリンタに印刷データを送信し（S127）、正常終了の通知を行なう（S128）。

【0053】印刷データは、ドキュメントサーバ116上の暗号化通信手段107からネットワークプリンタ117上の暗号化通信手段110を経由してプリンタ制御手段112に渡される。

【0054】ネットワークプリンタにおける出力までのプロセスの詳細は、図4のプリンタ制御手段処理のフローチャートに記されているので、これを参照しながら説明する。

【0055】ネットワークプリンタでは、前記したようにドキュメントサーバからの印刷データ受信に先立ってサーバ・プリンタ相互認証を行なっている（S140）。次にドキュメントサーバから認証結果を受信し（S141）、認証が失敗（S142のno）すればそのまま処理を終了する。認証が成功（S142のyes）すれば、プリンタ制御手段112は、印刷データを受信し（S143）、印刷手段113に印刷データを渡す。印刷手段113は印刷を実行し（S144）、印刷終了後に印刷終了通知（S145）を行なって処理を終了する。

【0056】以上のクライアント、ドキュメントサーバ、ネットワークプリンタの相互の通信プロトコルを図2に示し、以下手順を追って説明を行なう。

【0057】まず、クライアントはドキュメントサーバに対してサーバ認証を行なう。サーバ認証が成功したならば、クライアントはユーザによって入力されたドキュメントURI、プリンタURI、ユーザ認証情報を印刷要求データとしてドキュメントサーバに印刷要求する。ドキュメントサーバでは、受信したユーザ認証情報に基づくユーザ認証を行ない、ユーザ認証が失敗（NG）したならば、印刷拒否通知（応答（NG））をクライアントに送って、処理を終了する。

【0058】ユーザ認証が成功（OK）したならば、ドキュメントサーバとネットワークプリンタ間で相互認証を行ない、認証が失敗（NG）したならば、ドキュメントサーバからクライアントに印刷拒否通知が送られて処理を終了する。認証が成功（OK）すれば、ドキュメントサーバはネットワークプリンタに印刷要求を行ない、ネットワークプリンタは印刷を受け付けたことをドキュ

メントサーバに返す。続いて、ドキュメントサーバはネットワークプリンタに印刷データを送信し、ネットワークプリンタは受信した印刷データを印刷する。印刷が終了したら、ネットワークプリンタは、ドキュメントサーバに印刷終了通知を行ない、処理を終了する。ドキュメントサーバは、印刷終了通知を受信したら、クライアントに対して印刷完了通知（応答（成功））を行ない、処理を終了する。

【0059】以上のように、ネットワークプリンタの公開鍵証明書に基づく認証と、安全なプリンタとして登録されているリストとの照合とを行えば、不適格なプリンタへの出力が避けられる。

【0060】なお、図3の印刷制御手段のフローチャートで、安全なプリンタリストとの照合（S123、S124）とプリンタ認証（S125、S126）は逆の順序で行っても支障ない。

【0061】（第2の実施例）上記第1の実施例では、ドキュメントサーバが安全なプリンタのリストを持つことによりプリンタの安全性の確認を行なう方式を説明したが、本実施例では、プリンタ認証に使用する公開鍵証明書の拡張部（extension）にプリンタの安全性のクラスを示す情報が記載されているものとし、これを使用してプリンタの安全性を確認する方式について説明する。

【0062】安全性のクラスを示す情報としては、例えば、ネットワークプリンタがICカードなどのカード読み取り器を有し、印刷した本人の身分証明用ICカードを挿入しないと印刷物を取り出せないような機構を備えている場合に、メーカーが公開し、安全性を保証しているプリンタのクラス名称として、Security-Class: "ClassA-Printer" とする場合などがこれにあたる。図7にこの例を図示する。また、同様に印刷後のデータをプリンタから消し去ってしまい、分解してハードディスク装置などをアクセスしてもデータを盗むことが困難であることをメーカーが保証するクラス名などもこのようなクラスを示す情報として利用できる。

【0063】図5は本発明における第2の実施例の機密情報印刷システムの構成図である。図6はこの構成におけるドキュメントサーバにおける印刷制御手段の処理のフローチャートである。

【0064】図5の機密情報印刷システムの構成図において、図1と同番号の要素は図1と同内容であるので説明を省略する。ドキュメントサーバ216において、記憶手段101に保有する情報が、安全なプリンタリスト102ではなく安全とみなすクラスのリスト201になっている。また、ネットワークプリンタ217の記憶手段に保有するプリンタ認証拡張情報203は、前記のようにプリンタの公開鍵証明書拡張部（extension）にプリンタの安全性のクラスを示す情報を追加した

プリンタの公開鍵証明書とこれと対応する秘密鍵から成るものである。

【0065】以下、第1の実施例と異なる部分を中心に、本実施例における処理を図6の印刷制御手段の処理のフローチャートを参照しながら説明する。

【0066】図6の印刷制御手段の処理のフローチャートにおいて、開始から印刷権限を持つユーザのリストと照合し、印刷権限を確認する(S121, S122)までは、図1と同じ処理である。

【0067】その後、サーバ・プリンタ相互認証をし(S125)、認証が成功しなかった場合(S126のno)、印刷制御手段202は、印刷拒否の通知をクライアントに行なって(S131)処理を終了する。

【0068】認証が成功した場合(S126のyes)には、サーバ・プリンタ相互認証の際に得られたプリンタ認証拡張情報203のプリンタの公開鍵証明書からextensionを取り出し、ここに記述されている情報(クラス)を、安全とみなすクラスのリスト201と照合する(S225)。指定されたネットワークプリンタが当該ドキュメントを出力してよいリストに含まれていない場合(S226のno)、印刷拒否の通知をクライアントに行なって(S130)、処理を終了する。指定されたネットワークプリンタが当該ドキュメントを出力してよいリストに含まれている場合(S226のyes)は、ネットワークプリンタに印刷データを送信し(S127)、正常終了の通知を行なう(S128)。

【0069】ネットワークプリンタにおける出力までのプロセスの詳細は、実施例1における図4のプリンタ制御手段の処理のフローチャートと同じであり、また、クライアント、ドキュメントサーバ、ネットワークプリンタの相互の通信プロトコルは図2と同じであるため、ここでの説明は省略する。

【0070】以上のように、ネットワークプリンタの公開鍵証明書に基づく認証と、公開鍵証明書のextensionに記述されている安全性のクラスを示す情報を用いて安全とみなすプリンタのクラスのリストとの照合とを行なえば、不適格なプリンタへの出力が避けられ、さらに、同じクラスに属するプリンタの記述は1つで済むため、安全とみなすプリンタのリストを使用する場合と比較して、プリンタの追加や削除といった手間を省くことができる。

【0071】(第3の実施例)本実施例では、第1の実施例と同様に、サーバが安全なプリンタリストを持ち、プリンタ認証後に、安全なプリンタであるか否かをリストと照合して確認する方式を、参照印刷の形態について説明する。

【0072】図8は本発明における第3の実施例の機密情報印刷システムの構成図である。図9は参照印刷のプロトコル図、図10、図11はこの構成におけるプリンタのプリンタ制御手段の処理のフローチャート、図12

はこの構成におけるサーバの印刷データ制御手段の処理のフローチャートである。

【0073】図8の機密情報印刷システムの構成図において、図1と同番号の要素は図1と同内容であるので説明を省略する。

【0074】ドキュメントサーバ316の印刷制御手段301の処理と、ネットワークプリンタ317のプリンタ制御手段302の処理と、クライアント318の印刷要求手段の処理の内容については後で詳しく説明する。

【0075】上述の構成よりなる実施例の動作を、順を追って詳細に説明する。クライアント318は印刷要求手段305を用いて、ユーザによって要求された印刷したいドキュメント、出力したいネットワークプリンタ、そのユーザによって入力されたドキュメントの印刷が許可されているユーザを認証するための情報などから印刷要求データを生成する。印刷したいドキュメントやネットワークプリンタは、例えばWEBサーバ上のURL/URIなどの形式で行なう。

【0076】ユーザ認証のための情報としては、例えばユーザ名とパスワードを使用することもできる。印刷要求手段305は、次にこれらの印刷要求データを暗号通信手段304およびネットワークプリンタ317の暗号通信手段303を経由して、プリンタ制御手段302に送る。

【0077】このプリンタ制御手段302におけるクライアント・プリンタ間の処理は図10のクライアント・プリンタ間の処理(a)に記されているので、これを参照しながら説明する。

【0078】初めにクライアントとネットワークプリンタ間でプリンタ認証を行なう。プリンタの認証は、クライアント318の暗号通信手段304とネットワークプリンタ317の暗号通信手段303を経由して行ない。プリンタ認証情報111を用いた公開鍵証明書に基づく認証を行なうことで実施する。

【0079】ネットワークプリンタは、プリンタ認証情報111をクライアントに送信し(S340)、クライアントから認証結果を受信する(S341)。認証が失敗(S342のno)ならばそのまま処理を終了する。認証が成功(S342のyes)したならばクライアントから印刷要求データを受信(S343)して、サーバ・プリンタ間の処理(A)に移る。

【0080】次にプリンタ制御手段302は、受け取った印刷要求データを暗号通信手段110およびドキュメントサーバ上の暗号通信手段107を経由してドキュメントサーバ316の印刷データ制御手段301に送り、印刷データを要求する。

【0081】このプリンタ制御手段302におけるプリンタ・サーバ間の処理は図11のプリンタ・サーバ間の処理(b)に記されているので、これを参照しながら説明する。

【0082】まず、ネットワークプリンタとドキュメントサーバ間においてプリンタ認証を行なう（S344、S345）。

【0083】本実施例では、プリンタの認証は単独に行なうものではなく、サーバ認証といっしょに行なう形で書かれているが、サーバのなりすましの排除を行わない場合は、サーバ認証を省略した形で行なうこともできる。

【0084】サーバ・プリンタの相互認証は、ドキュメントサーバ316の暗号通信手段107とネットワークプリンタ317の暗号通信手段110を経由して、サーバ認証情報104とプリンタ認証情報111を用いた公開鍵証明書に基づく認証を相互に行なうことで実施する。この詳細については、従来の技術にあげた参考文献を参照されたい。

【0085】また、上記の説明で、暗号通信手段107、110、303、304については特に指定しなかったが、公知技術のSSLやTLSを使用してTCP/IPによる通信を行なう場合、SSL/TLSでは暗号通信を行なう前にサーバ認証（この場合クライアントのプリンタ認証ではネットワークプリンタ、プリンタ・サーバ相互認証ではドキュメントサーバ）を、オプションとしてクライアント（この場合だとネットワークプリンタ）認証を行なうことができるので、プリンタ制御手段302及び印刷データ制御手段301での処理を省略することも可能である。

【0086】さて、ネットワークプリンタは、サーバ・プリンタの相互認証が成功しなかった場合（S346のno）、処理を終了する。サーバ・プリンタの相互認証が成功した場合（S346のyes）には、ドキュメントサーバに印刷要求データを送ることで印刷データを要求する（S347）。次にドキュメントサーバからユーザ認証結果を受信し（S348）、ユーザ認証が成功しなかった場合（S349のno）、処理を終了する。ユーザ認証が成功した場合（S349のyes）には、印刷データを受信し（S350）、印刷データを印刷手段113に渡す（S351）。印刷が終了したらネットワークプリンタは、クライアントに印刷終了を通知して（S352）、処理を終了する。

【0087】また、印刷データ制御手段301におけるプロセスは、図12の印刷データ制御手段の処理のフローチャートに記されているので、これを参照しながら説明する。

【0088】ドキュメントサーバは、ネットワークプリンタから印刷データを要求されたら、前記のサーバ・プリンタ相互認証を行なう（S320）。サーバ・プリンタの相互認証が成功しなかった場合（S321のno）、印刷データ制御手段301は印刷拒否の通知をプリンタ経由でクライアントに行なって（S329）、処理を終了する。サーバ・プリンタの相互認証が成功した

場合（S321のyes）には、印刷データ制御手段301は、印刷要求データから印刷先のネットワークプリンタのURIを取り出し、安全なプリンタのリスト102と照合する（S322）。ネットワークプリンタが当該ドキュメントを出力してよいリストに含まれていない場合（S323のno）、印刷拒否の通知をプリンタ経由でクライアントに行なって（S330）、処理を終了する。ネットワークプリンタが当該ドキュメントを出力してよいリストに含まれている場合（S323のyes）は、印刷データ制御手段301は、受け取った印刷要求データから、ドキュメントURIとユーザ認証情報を抽出する（S324）。次に印刷データ制御手段301は、ユーザ認証情報に基づいてユーザの認証を行ない、さらに印刷権限をもつユーザのリスト103とユーザ名を照合して、当該ドキュメントの印刷権があるか確認する（S325）。ユーザ認証が失敗しているか、印刷権がないと判断（S326のno）された場合には、印刷拒否の通知をプリンタ経由でクライアントに行なって（S331）、処理を終了する。ユーザ認証と印刷権が確認（S326のyes）された場合は、ネットワークプリンタに印刷データを送信し（S327）、正常終了の通知を行ない（S328）、処理を終了する。

【0089】以上のクライアント、ドキュメントサーバ、ネットワークプリンタの相互の通信プロトコルを図9に示し、以下手順を追って説明を行なう。

【0090】まず、クライアントはネットワークプリンタに対してプリンタ認証を行なう。プリンタ認証が成功したならば、クライアントはドキュメントURIとユーザによって入力されたユーザ認証情報を印刷要求データとしてネットワークプリンタに送信する。ネットワークプリンタとドキュメントサーバ間で相互認証を行ない、認証が失敗（NG）したならば、クライアントに印刷拒否通知が送られて処理を終了する。認証が成功（OK）すれば、ネットワークプリンタはドキュメントサーバに印刷データを要求する。ドキュメントサーバでは、受信したユーザ認証情報に基づくユーザ認証を行ない、ユーザ認証が失敗（NG）したならば、印刷拒否通知（応答（NG））をプリンタ経由でクライアントに通知して、処理を終了する。ユーザ認証が成功（OK）したならば、ドキュメントサーバはネットワークプリンタに印刷データを送信する。ネットワークプリンタは受信した印刷データを印刷し、印刷が終了したならば、クライアントに印刷完了通知（応答（成功））を行ない、処理を終了する。

【0091】以上のように、ネットワークプリンタの公開鍵証明書に基づく認証と、安全なプリンタとして登録されているリストとの照合とを行えば、不適格なプリンタへの出力が避けられる。

【0092】（第4の実施例）本実施例では、参照印刷の形態で起こりうるユーザ認証情報の盗用への対策を説

明する。

【0093】図13は本発明の第4の実施例の機密情報印刷システムの構成図である。図中、ドキュメントサーバ516中の印刷データ制御手段501は、図8の参照印刷形態の実施例3の印刷データ制御手段の処理内容を変更したものである。変更された処理内容は図15の印刷データ制御手段の処理のフローチャートに記載されている。

【0094】また、クライアント518中の印刷要求データ暗号化手段502と印刷要求手段503は本実施例に特有の処理を行っており、その処理内容については後述する。

【0095】ドキュメントサーバ516中の101, 102, 103, 104, 106, 107、およびネットワークプリンタ517中の110, 111, 113は図1の同番号要素と、また、ネットワークプリンタ517中の302, 303およびクライアント518中の304は図8の同番号要素と同じものであるので、説明を省略する。

【0096】次に上述の構成よりなる実施例の動作を、実施例3との差異を中心に詳述する。前述のように、参照印刷の形態においては、ユーザ認証情報は必ずネットワークプリンタを経由してドキュメントサーバに送られることから、通信路の盗聴やネットワークプリンタのなりすましによって得たユーザ認証情報を再使用することによるドキュメントの再取得や、他のドキュメントのアクセスへのユーザ認証情報の流用という危険が存在する。

【0097】これに対応するため、本実施例のクライアント518は印刷要求手段503を用いて印刷要求データを生成する際に、印刷要求データ暗号化手段502を用いて印刷要求データの少なくとも一部をドキュメントサーバのみが復号できるように暗号化する。

【0098】この暗号化の方法としては、ドキュメントサーバの公開鍵証明書に含まれる公開鍵（事前に入手しておくか、この時点でドキュメントサーバと前記のSSL/TLSなどで接続すれば入手可能）を使用した暗号化があげられる。公開鍵暗号の性質として広く知られていることであるが、これは、特定の公開鍵で暗号化されたデータは、その公開鍵と対応する秘密鍵でのみ復号できるという性質を利用したものであり、ドキュメントサーバの公開鍵で暗号化したデータは、ドキュメントサーバのみが保有している秘密鍵のみで復号できる。

【0099】暗号化する印刷要求データとしては、ユーザ認証の方式がユーザ名・パスワードであれば、少なくともパスワードを暗号化すべきであるが、その他にも、他のドキュメントのアクセスにこの印刷要求データが流用されるのを防止するためにドキュメントURIを含めたり、他のネットワークプリンタからの利用を防止するためにプリンタURIを含めることが有効である。

【0100】また、なりすましたネットワークプリンタが同一の印刷要求データを何度も利用して複数の印刷を行うことを防止するには、印刷要求データを生成した時刻データやシリアルナンバー、乱数など、特定の印刷要求データを他と識別できるデータを添付して暗号化することも有効である。暗号化した印刷データの例を図16に示す。

【0101】さて、印刷要求手段503によって生成された印刷要求データはネットワークプリンタ517を経由してドキュメントサーバ516に送られるが、ネットワークプリンタ517上の処理は、実施例3の図11のステップS347の印刷データ要求の際に送付する印刷要求データの一部が暗号化されているのみで、その処理内容に変化はない。図14の参照印刷のプロトコル(5)に、暗号化したユーザ認証情報が送られる様子を示す。

【0102】次にドキュメントサーバ516における処理を、図15の印刷データ制御手段の処理のフローチャートを参照しつつ説明する。図15と実施例3の図12との差異は、S524（図12ではS324）のステップで、クライアント518で少なくとも一部が暗号化された印刷要求データを、サーバ認証情報104の一部としてドキュメントサーバのみが保有しているドキュメントサーバの秘密鍵を用いて復号した後、必要なデータを抽出する部分のみである。

【0103】なおこの際、印刷要求データに上で述べたドキュメントURIやプリンタURI、印刷要求生成時刻などが含まれている場合は、印刷データを要求してきたプリンタとプリンタURIの比較を行ったり、印刷要求されたドキュメントとドキュメントURIとを比較することによって、印刷要求データの盗用・流用を防止することができる。また印刷要求データ生成時刻から特定の短い時間の間だけ、印刷要求データが有効であるような制御をドキュメントサーバで行ったり、特定の印刷要求データを識別するのに使用できる印刷要求生成時刻やシリアルナンバーのようなデータを用いれば、なりすましたネットワークプリンタが同じ印刷要求データを複数回使用することも防止可能となる。

【0104】以上、説明したように、本実施例によれば、参照印刷の形態で起こりうるユーザ認証情報の盗用もしくは再利用を防止することができ、ネットワークプリンタの認証および安全なプリンタの確認とあいまって、当該ドキュメントを印刷する権限のある正当なユーザにだけ、安全なプリンタへの印刷を可能とすることができる。

【0105】（第5の実施例）本実施例では、参照印刷の形態で起こりうるユーザ認証情報の盗用への対策として、ユーザの公開鍵証明書を使用する方法について説明する。

【0106】図17は本発明の第5の実施例の機密情報

印刷システムの構成図である。図中、ドキュメントサーバ616中の印刷データ制御手段602は、図13の参照印刷形態の実施例4の印刷データ制御手段501の処理内容を変更したものである。変更された処理内容は図19の印刷データ制御手段の処理のフローチャートに記載されている。

【0107】また印刷権限を持つクラスのリスト601は、図13の印刷権限を持つユーザのリスト103に代わるものである。この内容および使用法は後述する。

【0108】また、クライアント618中の記憶手段605に格納されているユーザ認証拡張情報603、および印刷要求手段604は本実施例に特有の処理を行っており、その内容および処理内容については後述する。また、印刷要求データ暗号化手段502は図13の同番号要素と同一のものである。

【0109】ドキュメントサーバ616中の101、102、104、106、107、およびネットワークプリンタ617中の110、111、113は図1の同番号要素と、また、ネットワークプリンタ617中の302、303およびクライアント618中の304は図8の同番号要素と同じものであるので、説明を省略する。

【0110】次に上述の構成よりなる実施例の動作を、実施例4との差異を中心に詳述する。実施例4では、ユーザ認証方式がユーザ名・パスワードである例について説明を行ったが、本実施例ではユーザの公開鍵証明書に基づくユーザ認証方式を採用している場合について説明する。

【0111】クライアント618の印刷要求手段604は、印刷すべきドキュメントURIや印刷先のネットワークプリンタURIなどの印刷要求データの入力を受けたあと、これら印刷要求データの一部もしくは全部、またはそれらのダイジェスト情報に対して、ユーザ認証拡張情報603に含まれる公開鍵証明書に対応した秘密鍵を使って、デジタル署名を生成する。(このデジタル署名は、後にドキュメントサーバ616上で印刷要求に含まれる印刷要求データを確認する際、これらが改竄されていないことの証明となる。)クライアント618の印刷要求手段604は、このデジタル署名を添付した印刷要求データを新たな印刷要求データとし、実施例4と同様に印刷要求データ暗号化手段502を用いてドキュメントサーバの公開鍵で暗号化して、ネットワークプリンタ617を経由してドキュメントサーバ616に送る。

【0112】なおドキュメントサーバのユーザ認証がLDAPなどのディレクトリサービスを用いて行われておらず、ユーザの公開鍵証明書が入手できない場合は、上記印刷要求データにデジタル署名とともに、ユーザの公開鍵証明書自体を添付してやればよい。印刷要求データとデジタル署名の例を図20に示す。

【0113】ネットワークプリンタ617上の処理は、実施例4と同様に(実施例4でも参照した、実施例3の

図11のステップS347の)印刷データを要求する際に送付する、印刷要求データの形式が実施例4と異なるのみで、その処理内容に変化はない。図18の参照印刷の Protokol (6) に、暗号化したユーザ認証拡張情報が送られる様子を示す。

【0114】ネットワークプリンタ617を経由して、印刷要求を受け取ったドキュメントサーバ616は、印刷データ制御手段602を用いて処理を行う。図19の印刷データ制御手段の処理のフローチャートがその内容であるが、この内容は実施例4の印刷データ制御手段501の処理内容とは、S622のユーザ認証と分岐S623と認証失敗による印刷拒否通知S631、およびS624、S625からなる印刷権限の確認部分で異なっている。

【0115】まずS622でユーザ認証を行う。ユーザ認証はユーザのデジタル署名の正しさを確認することで行われる。サーバの公開鍵で復号された印刷要求データからドキュメントURIやプリンタURIなど、クライアント618の印刷要求手段604で生成したデジタル署名の対象であるデータを抽出し(ダイジェスト情報を使用している場合は、これらのダイジェスト情報を作成して)、同じく復号された印刷要求データから抽出されたデジタル署名とこれが対応しているか否かをユーザの公開鍵を用いて確認する(S622)。

【0116】ここでユーザの公開鍵は、ドキュメントサーバのユーザ認証がLDAPなどのディレクトリサービスを用いて行われていればそこから、そうでない場合は、上記印刷要求データにデジタル署名とともに添付されているユーザの公開鍵証明書から抽出して使用すればよい。デジタル署名と対象データの対応が取れず、認証が失敗した場合(S623のno)は印刷拒否通知(認証失敗)S631を行い、処理は終了する。認証が成功した場合(S623のyes)は、S624、S625のドキュメントの印刷権限の確認に移る。

【0117】実施例4ではドキュメントの印刷権限の確認はドキュメントと関連付けられた印刷権限を持つユーザのリストとの照合であったが、本実施例ではユーザの公開鍵証明書の拡張部に記された特定のユーザのクラスを使用する方法を用いている。ここで、クライアント618のユーザ認証拡張情報603に含まれるユーザの公開鍵証明書の拡張部にはドキュメントのアクセス権にかかわるクラス名が記入されているものとし、これがドキュメントに関連付けられた印刷を許可されたクラスのリスト601を満たす場合、印刷権ありとなる。アクセス権にかかわるクラス名としてはたとえば職制や職務上の担当などがあげられる。

【0118】図21にユーザの所属組織などが発行した拡張部付きのユーザの公開鍵証明書の例を示すが、この例ではユーザの職制が部長クラスであることを示しており、ドキュメントサーバ上で部長以上の印刷を許可する

機密情報についてユーザ認証成功となる。

【0119】ステップS624では、印刷要求データの一部として送られてきたユーザの公開鍵証明書の拡張部を抽出し、ユーザのアクセス権にかかわるクラス名を得る。次にS625は、ドキュメントサーバ616の印刷権限を持つクラスのリスト601とこの情報とを照合し、印刷権限を確認する。以降の処理は実施例4と同じである。

【0120】本方法の利点としては、ユーザ名そのものではなく、ユーザのクラスに対して印刷権限が設定されるため、ドキュメントに関連付けられた印刷を許可されたクラスのリストの管理の手間が小さくなることがあげられる。

【0121】以上説明したように、本実施例によれば、ドキュメントサーバの公開鍵による印刷要求データの暗号化に加え、ユーザの公開鍵証明書を用いた認証とデジタル署名により、印刷要求データが偽造あるいは流用される危険性をさらに小さくすることができ、参照印刷の形態で起こりうるユーザ認証情報の盗用もしくは再利用を防止することができる。また、ネットワークプリンタの認証および安全なプリンタの確認とあいまって、当該ドキュメントを印刷する権限のある正当なユーザにだけ、安全なプリンタへの印刷を可能とすることができる。

【0122】なお、クライアント618の印刷要求手段604は、デジタル署名を添付した印刷要求データを、印刷要求データ暗号化手段502を用いてドキュメントサーバの公開鍵で暗号化して送っているが、実施例4とは異なり、本実施例では印刷要求データにはデジタル署名がなされていることから偽造は困難であると考えられる。従って、なりすましたネットワークプリンタが印刷要求データを復号できないことは必ずしも必要ではなく、クライアントにおける印刷要求データのドキュメントサーバの公開鍵による暗号化と、ドキュメントサーバにおける復号の処理は省略することも可能である。

【0123】また、実施例4および実施例5で示した印刷要求データ（あるいはユーザ認証情報）の盗用もしくは再利用を防止する手法は、実施例2で示した安全なプリンタの確認に、ドキュメントに対応した安全クラスを使用する方法と組み合わせることも可能であり、これらの組み合わせによっても、当該ドキュメントを印刷する権限のある正当なユーザにのみ、安全なプリンタへの印刷を可能とするという目的を達成することができる。

【0124】以上の通り、印刷に先立って、当該ネットワークプリンタの認証を行い、正当性が確認されたプリンタについて、そのドキュメントの印刷許可があるかどうかの確認を行う必要がある。このためには、ネットワークプリンタ内にそのプリンタを特定できる公開鍵証明書とこれに対応する秘密鍵を持たせ、ドキュメントデータの送信に先立って、公開鍵証明書に基づくプリンタの

認証を行う。さらに、ドキュメントサーバ上に、ドキュメントの適切な分類と対応した安全なネットワークプリンタのリストを持たせ、これと認証したネットワークプリンタとの照合を行う。以上により、上記課題が解決できる。

【0125】ドキュメントデータの送信に先立って、ネットワークプリンタの公開鍵証明書に基づく認証と、ドキュメントの適切な分類と対応したプリンタの安全性の確認を行なうことにより、ネットワークプリンタのなりすましを防止し、安全なプリンタのみへの印刷を可能とすることができる。

【0126】また、ユーザクライアントはユーザ認証情報を含む印刷要求データの少なくとも一部を、ドキュメントサーバのみが復号可能なように暗号化して送る。しかる後に、ネットワークプリンタを経由して、一部を暗号化した印刷要求データを受け取ったドキュメントサーバが、当該ドキュメントのユーザの印刷権限の確認を行う際、印刷要求の偽造が行われていないことを確認することにより、ユーザ認証情報や印刷を指示する情報が盗用され、ドキュメントの再取得や他のドキュメントのアクセスに流用されることを防止することができる。

【0127】ドキュメントサーバ上で管理されている機密性を含むドキュメントを、ネットワークに接続されたプリンタに印刷するシステムにおいて、参照印刷の形態で起こりうるユーザ認証情報の盗用もしくは再利用を防止することができ、ネットワークプリンタの認証および安全なプリンタの確認とあいまって、当該ドキュメントを印刷する権限のある正当なユーザにだけ、安全なプリンタへの印刷を可能とすることができる。

【0128】本実施例は、コンピュータがプログラムを実行することによって実現することができる。また、プログラムをコンピュータに供給するための手段、例えばかかるプログラムを記録したCD-ROM等の記録媒体又はかかるプログラムを伝送するインターネット等の伝送媒体も本発明の実施例として適用することができる。上記のプログラム、記録媒体及び伝送媒体は、本発明の範疇に含まれる。

【0129】なお、上記実施例は、何れも本発明を実施するにあたっての具体化のほんの一例を示したものに過ぎず、これらによって本発明の技術的範囲が限定的に解釈されてはならないものである。すなわち、本発明はその技術思想、またはその主要な特徴から逸脱することなく、様々な形で実施することができる。

【0130】

【発明の効果】以上説明したように本発明によれば、プリンタのなりすましを防止し、安全なプリンタへのみ印刷することができる。また、参照印刷の形態において、プリンタを経由してドキュメントサーバに送られるユーザ認証情報が他の目的に使用できないようにすることができる。



## 【図面の簡単な説明】

【図 1】本発明の実施例 1 による機密情報印刷システムの構成図である。

【図 2】サーバ印刷のプロトコルを示す図である。

【図 3】実施例 1 における印刷制御手段の処理を説明するフローチャートである。

【図 4】実施例 1 におけるプリンタ制御手段の処理を説明するフローチャートである。

【図 5】本発明の実施例 2 による機密情報印刷システムの構成図である。

【図 6】実施例 2 における印刷制御手段の処理を説明するフローチャートである。

【図 7】拡張されたプリンタの公開鍵証明書を示す図である。

【図 8】本発明の実施例 3 による機密情報印刷システムの構成図である。

【図 9】参照印刷のプロトコルを示す図である。

【図 10】実施例 3 におけるプリンタ制御手段の処理を説明するフローチャートである。

【図 11】実施例 3 におけるプリンタ制御手段の処理を説明するフローチャートである。

【図 12】実施例 3 における印刷データ制御手段の処理を説明するフローチャートである。

【図 13】本発明の実施例 4 による機密情報印刷システムの構成図である。

【図 14】参照印刷のプロトコルを示す図である。

【図 15】実施例 4 における印刷データ制御手段の処理を説明するフローチャートである。

【図 16】実施例 4 におけるクライアントが生成する印刷要求データを説明する図である。

【図 17】本発明の実施例 5 による機密情報印刷システムの構成図である。

【図 18】参照印刷のプロトコルを示す図である。

【図 19】実施例 5 における印刷データ制御手段の処理を説明するフローチャートである。

【図 20】実施例 5 におけるユーザの公開鍵証明書を用いる場合の印刷要求データを説明する図である。

【図 21】拡張部付きのユーザの公開鍵証明書を示す図である。

【図 22】印刷の形態を示す図である。

【図 23】機密情報印刷の危険性を示す図である。

## 【符号の説明】

101 記憶手段

103 印刷権限を持つユーザのリスト

105 印刷制御手段（サーバ印刷）

107 暗号通信手段

109 暗号通信手段

111 記憶手段

113 印刷手段

115 印刷要求手段（サーバ印刷）

117 ネットワークプリンタ

201 安全とみなすクラスのリスト

203 プリンタ認証拡張情報

217 ネットワークプリンタ

301 印刷データ制御手段

303 暗号通信手段

305 印刷要求手段（参照印刷）

317 ネットワークプリンタ

501 印刷データ制御手段

503 印刷要求手段（参照印刷）

517 ネットワークプリンタ

601 印刷権限を持つクラスのリスト

603 ユーザ認証拡張情報

605 記憶手段

617 ネットワークプリンタ

102 安全なプリンクリスト

104 サーバ認証情報

106 ドキュメント保存手段

108 印刷要求受付手段

110 暗号通信手段

112 プリンタ制御手段（サーバ印刷）

114 暗号通信手段

116 ドキュメントサーバ

118 クライアント

202 印刷制御手段

216 ドキュメントサーバ

218 クライアント

302 プリンタ制御手段（参照印刷）

304 暗号通信手段

316 ドキュメントサーバ

318 クライアント

502 印刷要求データ暗号化手段

516 ドキュメントサーバ

518 クライアント

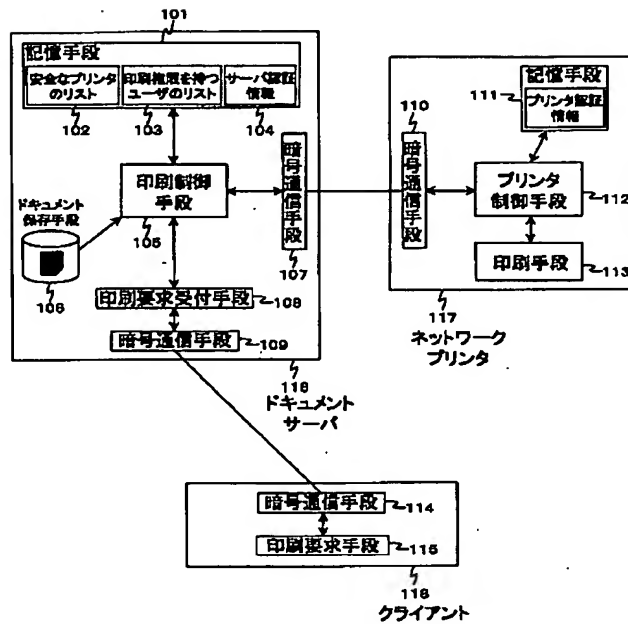
602 印刷データ制御手段

604 印刷要求手段（参照印刷）

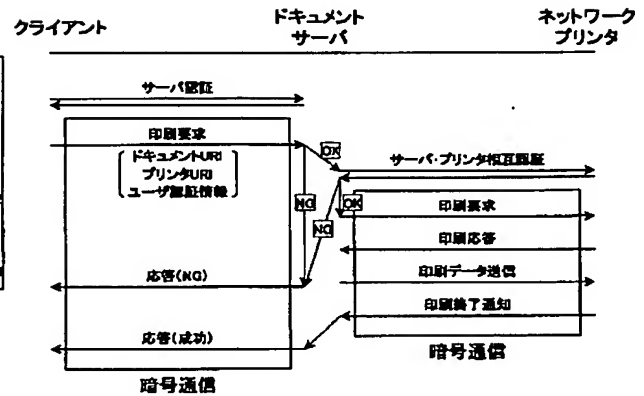
616 ドキュメントサーバ

618 クライアント

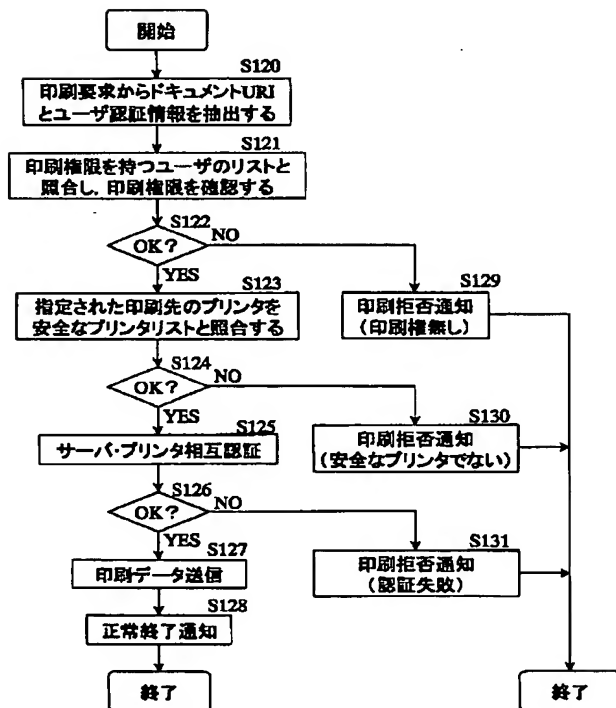
【図1】



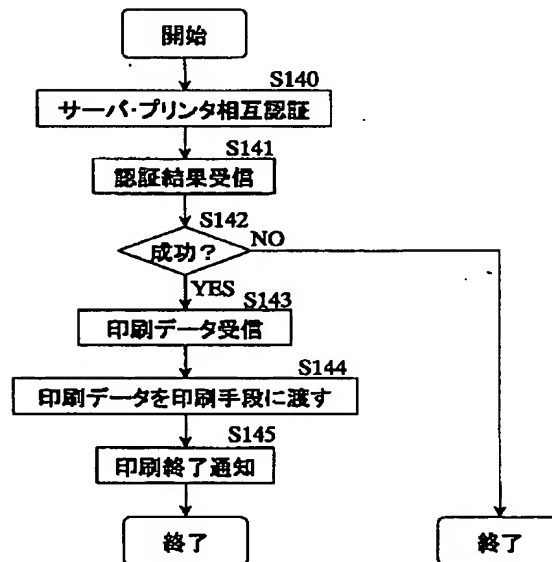
【図2】



【図3】

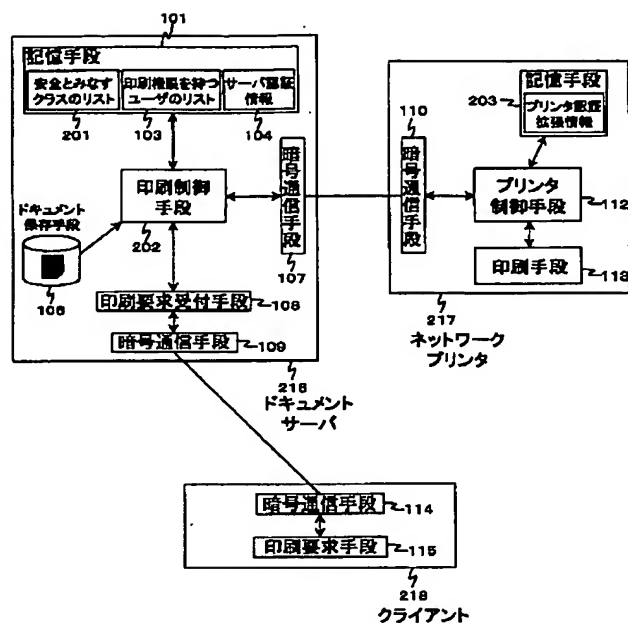


【図4】

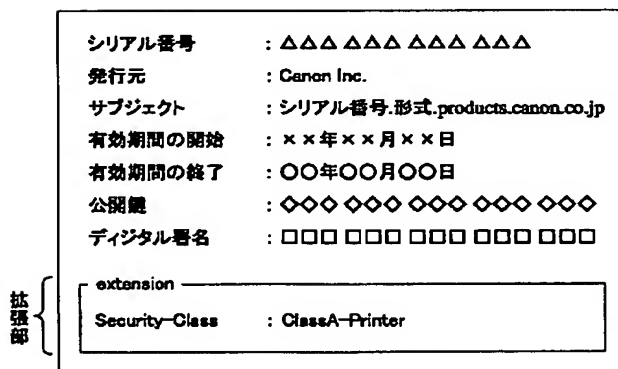




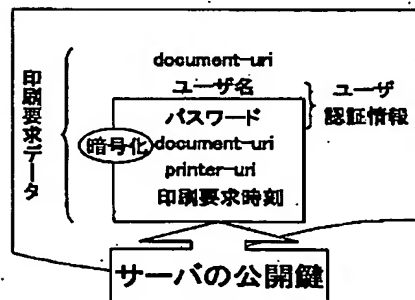
【図5】



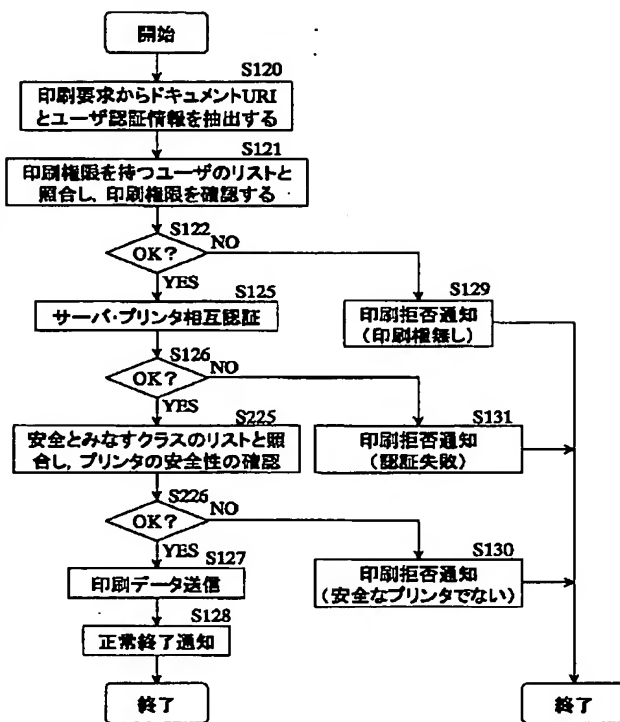
【図7】



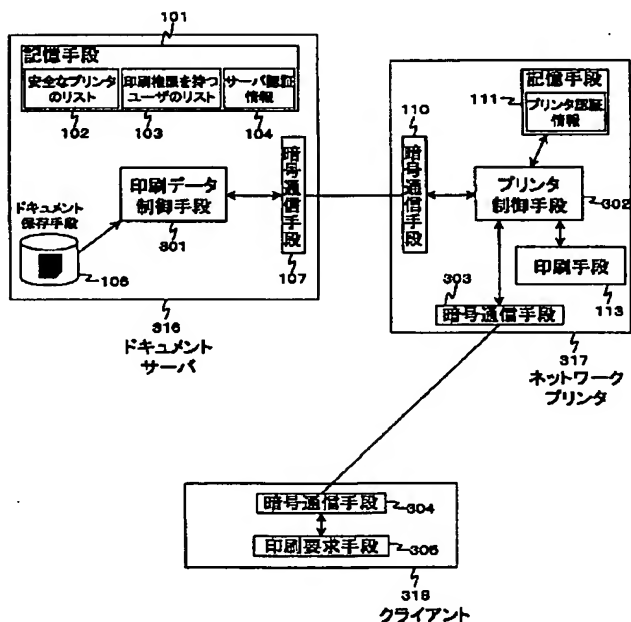
【図16】



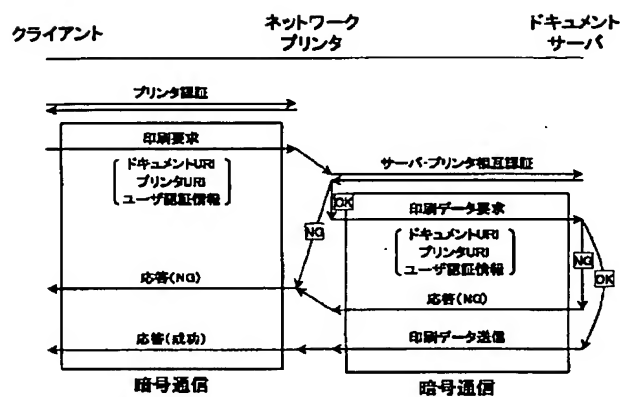
【図6】



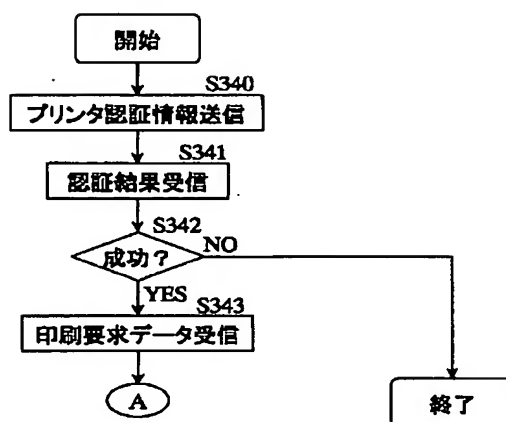
【図8】



【図9】

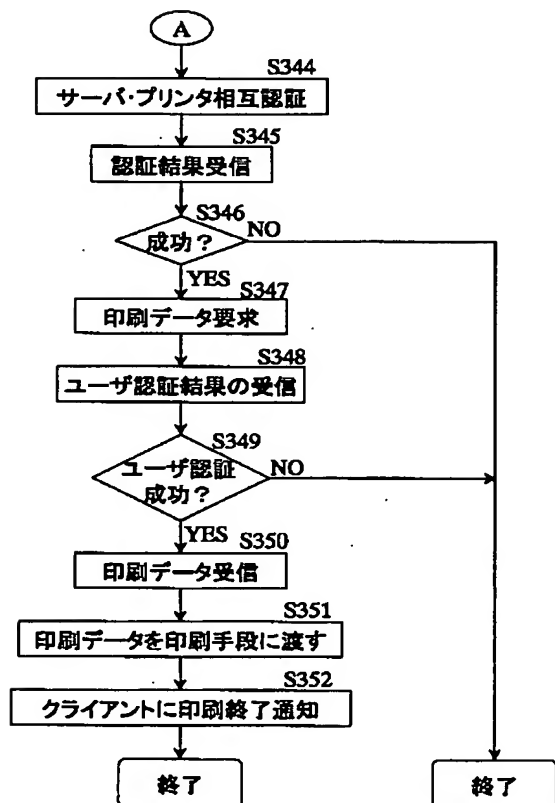


【図10】



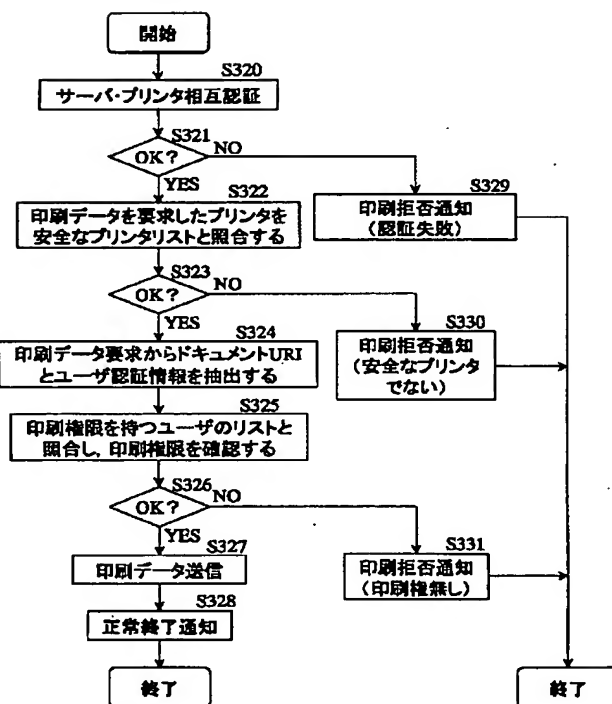
クライアント・プリンタ間の処理

【図11】

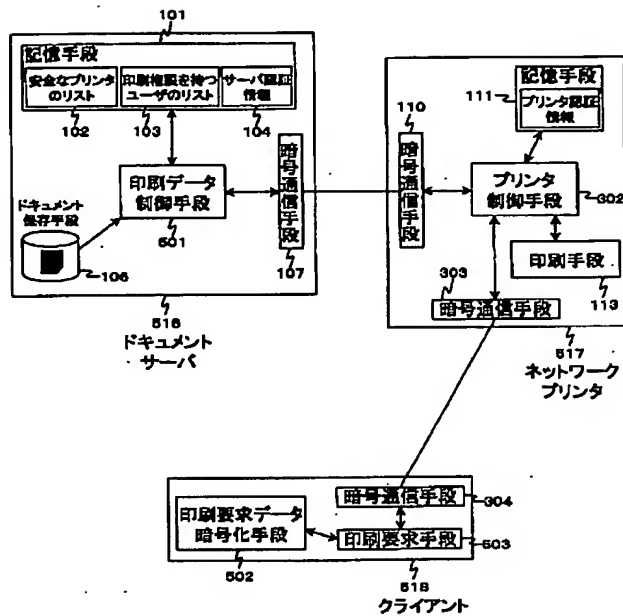


プリンタ・サーバ間の処理

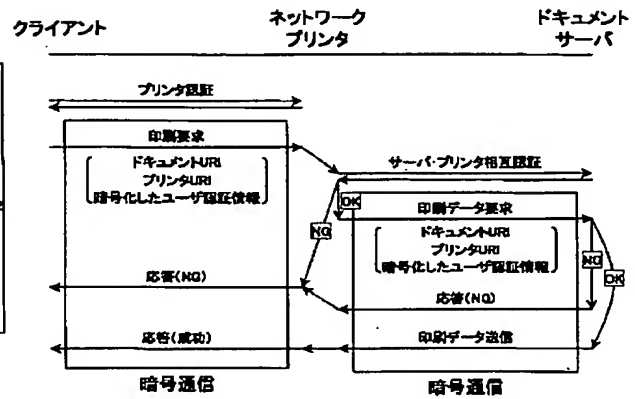
【図12】



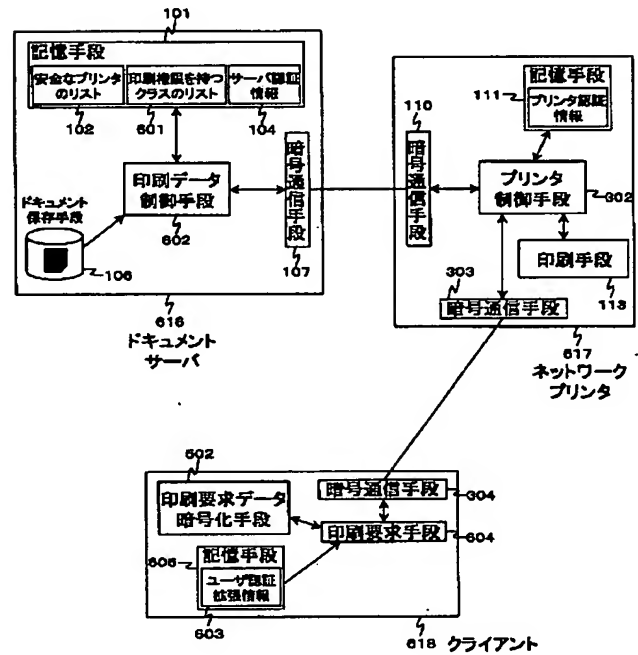
【図13】



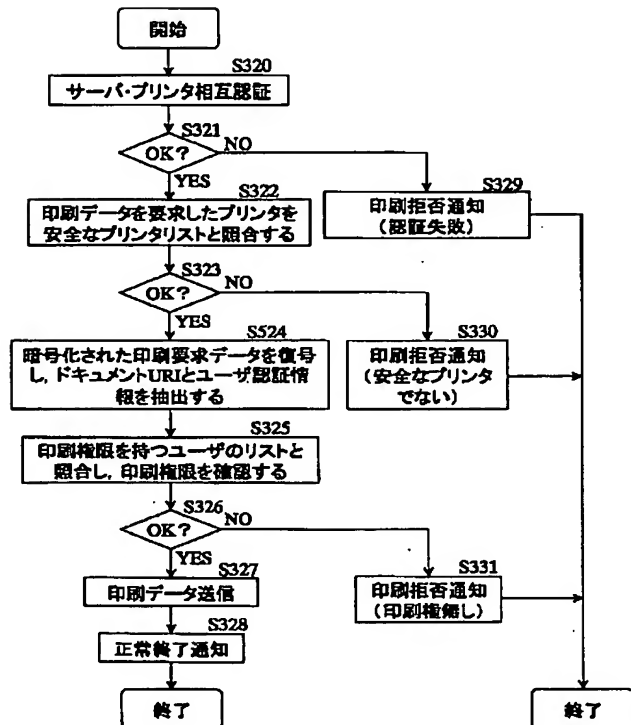
【図14】



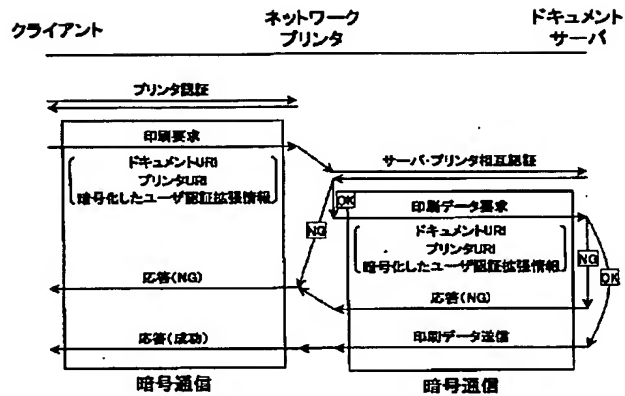
【図17】



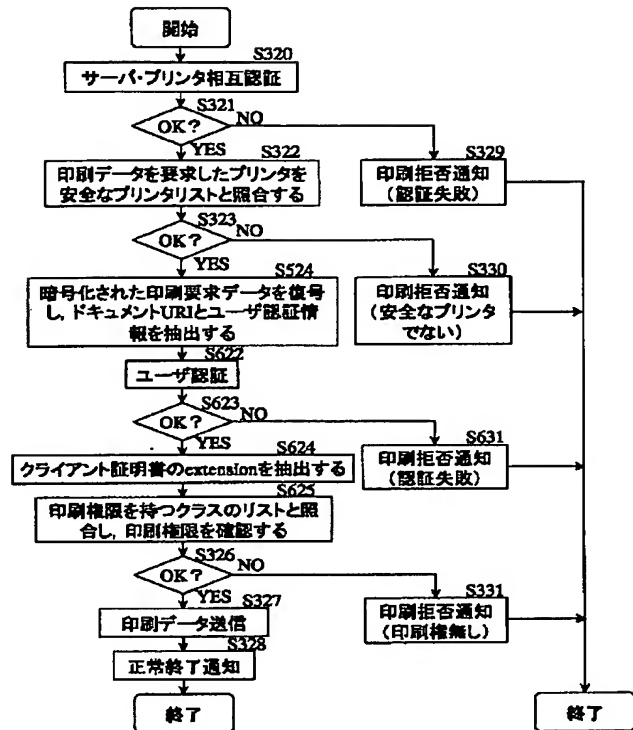
【図15】



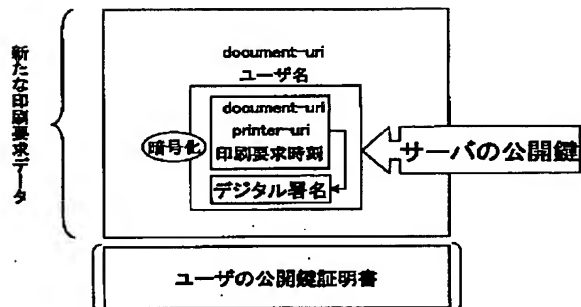
【図18】



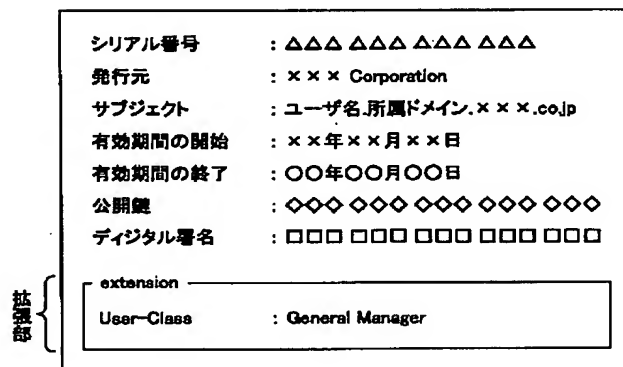
【図19】



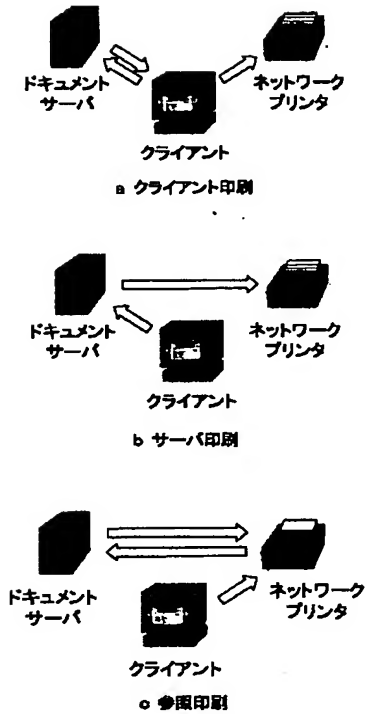
【図20】



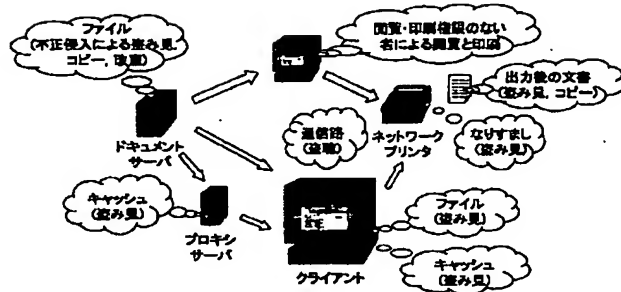
【図21】



【图 22】



【☒23】



フロントページの続き

Fターム(参考)	2C061	AP01	CL08	CL10	HH01	HJ08
		HN23	HV01	HV32	HV44	HX10
	5B021	AA01	EE02	EE04	NN18	
	5B085	AA08	AE02	AE03	AE04	
	5J104	AA07	KA01	KA05	NA02	PA07